PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6: H04L 9/32, G06F 17/30, H04K 1/00 — A1

(11) International Publication Number: WO 98/17029

(43) International Publication Date: 23 April 1998 (23.04.98)

(21) International Application Number: PCT/SE97/01713

(22) International Filing Date: 14 October 1997 (14.10.97)

(30) Priority Data:
9603825-2 17 October 1996 (17.10.96) SE

(71) Applicant: TELIA AB [SE/SE]; Mårbackagatan 11, S-123 86 Farsta (SE).

(72) Inventors: SVENSSON, Claes; Folkungagatan 16 A, S-753 36 Uppsala (SE). SVENSSON, Anders; Flogstavägen 41 B, S-752 73 Uppsala (SE).

(74) Agent: MAYER, Till; Telia Research AB, Rudsjöterrassen 2, S-136 80 Haninge (SE).

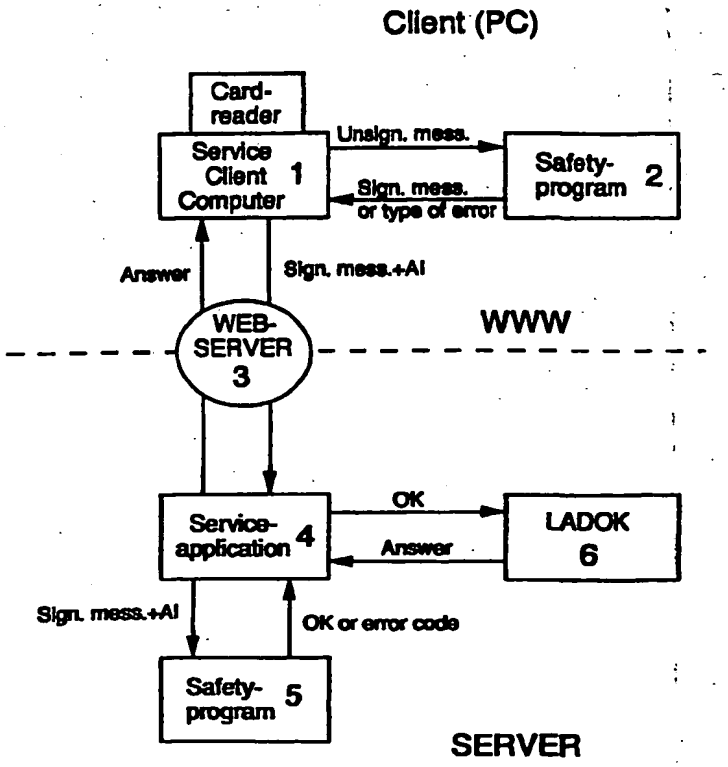
(81) Designated States: NO, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: TRANSFER OF SIGNED AND ENCRYPTED INFORMATION

(57) Abstract

The invention relates to a device and a method at a telecommunications system and a data communications system which makes possible signing and encryption of the information which is transmitted between a transmitting and a receiving equipment in said system. The invention is briefly characterized in a software for signing and encryption by means of smart cards which are linked together with a software which can show text, data entry fields, buttons, etc. This program is utilized as a plug-in unit or a Java-unit in a WWW-browser. Before the information is shown to the user, or is transmitted from the user, encryption functions can be applied to the information. All internal communication related to the safety on the local PC will by that be needless, by all necessary information processing being performed in said plug-in unit. All extra steps in the signalling process is by that concealed from the user and intruders, if any.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

TRANSFER OF SIGNED AND ENCRYPTED INFORMATION

FIELD OF THE INVENTION

The present invention relates to a device and a method at a telecommunications system or data communications system which makes possible signing and encryption of information which is transmitted between a transmitting equipment and a receiving equipment.

PRIOR ART

The increased interest among the public in IT and especially Internet has resulted in that many companies och private persons want to carry on trade via Internet.

The problem that will arise when someone wants to sell anything via Internet is how payment communication and trade communication shall be made in a reliable and to unauthorized persons uninterpretable way.

Another situation of use where it is important with safe information transfer, where no unauthorized persons shall have possibility to acquaint themselves with the contents of transmitted information, is when certain persons/companies have authority to read certain programs or databases in a communications system (for instance Internet).

The problem above is solved by means of encryption of the information which is transmitted and verification of the identity of the users who are transmitting the information. The encryption and signing of today via Internet, however, is imperfect because there occur unneccessary communication of not encrypted information

between processors and servers before the information is encrypted.

If one for instance today wants to sign and encrypt a document in Internet, where a web-server is run locally towards the client machine, the document is transmitted to the server where a CGI (Common Gateway Interface)-program performs signing/encryption.

After that a newly made page is transmitted from the CGI-program to the Web-browser (Web-reader) where one acknowledges the transmission of data from the machine.

In order to find out whether the prior art describes encryption and signing via Internet, a preliminary investigation was made, at which the following documents were found:

Document 1: EP,A1, 693 836
2: EP,A2, 702 477
3: WO,A1, 96/05681
4: WO,A1, 93/15581
5: DE,A1, 44 14 553
6: EP,A1, 696 121 (abstract + figure)

Document 1 relates to a method and equipment for managing of code keys at transmission of encrypted information over Internet. See especially "Summary of the invention", "Application of the present Invention to Site Firewalls" (column 13, Figure 6-10) and "User Authentication" (column 17).

Document 2 relates to a system for automatic encryption and decryption of data packets transmitted between "sites" on Internet or other data networks. See especially

"Abstract", "Description" (page 1) and "APPENDIX A" (page 8).

Document 3 describes a device and a method for indentification and authentication at establishing of connection to local data networks via for instance Internet. The document does not deal with encrypted transmission. See especially "Abstract" and Figure 1 and 3 with belonging text.

Document 4 describes a method, device and arrangements for encrypted transmission of information between interconnected networks, preferably by means of the protocol TCP/IP. See "Abstract" and Figure 1 and 2 with belonging text.

Document 5 describes determination of authenticity of subscribers´equipment by means of TCP/IP. The document does not deal with encrypted transmission.

The above found documents are, however, marred by the same problem as has been described above regarding encryption and signing of document via Internet.

SUMMARY OF THE INVENTION

The aim of the present invention consequently is to clear away above mentioned problem and provide a very safe communication via an information carrying network such as, for instance, Internet.

This aim is achieved by a device and method which is characterized in that a software for signing and encryption by means of smart cards or by means of software is linked together with a software which shows text, data entry fields, buttons and icons etc, which linked-up program is utilized as a plug-in unit or Java-unit in a browser, at

which all information to/from the user is decrypted/encrypted in said plug-in unit or said Java-unit.

An advantage with this is that all internal communication regarding the security on the local PC by that becomes needlesss, because all necessary processing of information is made in the plug-in unit or Java-unit; supporting programs executing as a part of the browser.

Another advantage is that all extra steps are concealed from the user and, if any, intruders. If delicate information shall be processed, then the Java- or plug-in unit program can encrypt everything that is going out, and decrypt everything that is coming in automatically. No text en clair will be transmitted between processes, not even on the local computer.

Because it is a "living" program that is executed in the browser, there is possibility to do so much more than in an ordinary HTML-form.

The program also can communicate over the network in the background, for instance for monitoring processes.

BRIEF DESCRIPTION OF THE DRAWING

In the following a more detailed description of the invention is given with reference to the only drawing.

Figure 1 describes schematically the verification procedure in the telecommunications system according to the present invention.

DETAILED DESCRIPTION OF AN EMBODIMENT OF THE INVENTION

The aim with the present invention is, as has been mentioned above, to effect a way to sign documents or

corresponding information electronically and to transmit and receive encrypted information over an information carrying communication network such as, for instance, Internet, and where said encryption respective signing shall be made by means of utilization of smart cards or by software which can cooperate with said network.

The aim above all is to make possible to transmit messages with personal signatures over Internet.

This of course can be used in a large number of different connections such as electronic banking, travel agencies, trade of different kinds or controlled access to databases which are made accessible via the network.

In this embodiment different services are described which are made accessible from KTH's (KTH = "Kungl. Tekniska Högskolan", i.e. "The Royal Institute of Technology") documentation system (LADOK) via Internet, provided that one has authorization to get access to these services.

Some abbreviations which will turn up continuously in the description now will be explained:

CA	Certification Authority
CGI	Common Gateway Interface
LADOC	Local, ADP-based Documentation System; KTH's equivalent to Uppsala University's UPPDOK.
MIME	Multipurpose Internet Mail Extensions
NSAPI	Netscape Server Application Programming Interface
URL	Uniform Resource Locator

The intention now will be described with reference to Figure 1.

The system according to the present invention consists of a computer 3, with a Web-server (called the server computer), one or more computers 1 with a WWW-browser and a card reader for smart cards. In addition all included computers 1 shall be connected to Internet. The client computer 1 includes a safety software 2.

Smart cards are personal cards with storage, processor, operative system etc. In these are the private key which is needed for signing and encryption and furthermore a certificate of X.509 standard. The certificate includes among other things the user's public key, CA's open key, information about the person etc. The card is an electronic identity document which in addition gives possibility to create personal electronic signatures which are unique to each person and card. The authenticity of the signature is possible to check by all levels which have access to the person's open key. This key can be obtained from a trusted authority on the network.

On the server side a service application 4 is conneced to the database LADOK 6, which service application includes a safety software 5.

The invention consequently implies to make services from LADOK accessible via Internet. Other services can, as has previously been mentioned, be arranged on the network with the same technology, for instance banking services, booking of journeys etc.

The service client 1 creates a signed message by an API-call to the safety software 2, where the message is given as parameters. The client 1 waits for answer which

can be: signed message or type of error. If a signed message arrives at the client 1, this shall be packed into a structure and transmitted over the network (WWW) to the service application 4 via the Web-server 3 for that machine. The service application 4 disassembles the structure and transmits the user identity and the signed message to the safety software 5 for verification. The verification shall give OK or error code. If OK is received, the application 4 shall transmit the message and user identity to LADOK 6 for preparation, otherwise user identity and message shall be logged. The application 4 waits for answer from LADOK´s 6 output or input process and returns this answer to the service client 1 via the network. The answer can be in ordinary text/html-form, or of some MIME-type, so a plug-in unit (not shown) can be started on the client side 1.

The answer shall include a description of how the work shall be possible to be extended for encryption in both directions.

In the started plug-in unit in the Web-browser at the server client 1 then all information which shall be transmitted to LADOK 6 is fed in, which information is encrypted directly in the plug-in unit. Signing of information/document is preferably made by a client utilizing an active card with personal code and a card reader connected to said plug-in unit. When encrypted information is coming in from LADOK 6 to the service client´s computer 1, the information is decrypted in the plug-in unit.

If, however, a general software is made which supports HTML-form management and certain extensions, then customer

adapted safety critical applications can be written with very small contribution of work. The client side gets one copy of the program (possibly automatically downloaded). The side which contains the extended form then starts the program to show the content. The program "parses" the extended HTML-form language and shows the content on the screen. When the user has made all the "feeding" and makes "submit", then all data is packed, signed and encrypted. No programming is needed for the clients and these moreover can use the same client software for a number of different applications.

On the server side there is a need of some programming, but with a Software Development Kit which has been developed (empty frame program), it is only the customer unique programming that needs to be added.

Extension implies that all communication over the network shall be encrypted.

The signatures shall be possible to be created by means of smart cards. If the deliveries of these cards are delayed, the signatures will, to begin with, be created in software.

In the following, preferred protocols and commands which are necessary to implement the embodiment will be discussed.

By network protocol is meant the protocol which is used between the Web-server and the Web-browser.

The service client 1 should transmit a tuple with the following appearance to the service application 4:

Application=SECUNET&Ver=versionnumber&...

for instance

Application=SECUNET&Ver=1.00&Type=Sign&UserCert=....&Msg=....&Signature=...

where

- Version number is a serial number of the type (in pseudo C-code) ("%D.0%2D", major, minor)
- Type is a string which describes the type of the message, can be
  - Normal
  - Sign
  - Encrypt
  - Sign&Encrypt
  - .. other types
- The user certificate is the certificate from the smart card.
- The messsage should be a URL-encoded string of all information that exists in the INPUT-fields in the form.
- Signature should be a URL-encoded string of the signature.

To the version number there shall be a mapping which decides the number of fields and what each field contains. This makes it easier to make changes in the protocol. There shall be a mapping for each type of protocol. If the receiving application cannot manage the type of protocol, it shall return an error code, preferably in HTML-form.

If URL-encoding is used and the protocol looks as above, existing CGI-programs can be utilized as basis for server applications. All binary data which shall be transmitted should be URL-encoded before it is transmitted

over the network. It should be realized that this applies to certificates, signatures and encrypted data.

The service client 1 shall extend the functionality of some type of WWW-browser making it manage signing, encryption, authentication and verification. As Netscape Navigator 2.0+ is expected to be widely spread, and as a lot of companies develop so called plug-in units for Navigator, that type of technology shall be used.

A plug-in unit shall be produced which can give possibility to read an input from the network (a URL), show it to a client, interact with the client, and finally transmit the result over the network, preferably in the same form as FORM (see the HTML-documentation) makes use of. The plug-in unit shall be associated with the MIME-type: application/x-secunet and file extensions: secunet and .sec if these are not engaged.

Registration of MIME-types shall be made at Netscape by the agency of Telia Promotor.

The input which the plug-in unit is expected to read shall consist of a subset of HTML. This language should contain the following commands (with approximately correspondning semantics as at HTML):

<P>

<HR>
<H1>...<H4>, </H1>... </H4>
<A...>, </A>
<SELECT...>
<FORM...>, </FORM>

and the following commands with extended semantics:

>INPUT...>

Input shall be able to take an extra parameter: EXTENDED. This parameter only need to have well-defined semantics about TYPE=SUBMIT when it indicates how the form shall be transmitted:

ENCRYPT

SIGN

SIGN and ENCRYPT

...possible future extensions

When corresponding button in the form is activated, suitable routines shall be called to process the indata which are in the form, before these are transmitted to the URL described in <FORM...>.

All options which exist to each HTML-command need not be implemented, but only those which are necessary to make communication, interaction with the user and signing to function.

The client shall be possible to be run under MS Windows 3.x and MS Windows 95/NT with Netscape Navigator. Which version that will be required on Navigator is to be determined by the application. Because Microsoft´s Internet Explorer has launched the same API as there is in Netscape Navigator, the plug-in unit probably will function with that software as well, but this is no demand.

To make it possible to find out whether a message which is coming to the plug-in unit is an encrypted or a common message, the following protocol identifier (or corresponding) should be used:

<HTML>

or

<SECUNET VERSION=ver TYPE=type>

where "ver" indicates the version number of the protocol and "type" indicates the type of the message, which for instance is encrypted or is signed. Lack of protocol identifier should be interpreted as if the message is of the type normal.

This is only for the purposse of facilitating a future extension of the system.

The service application 4 shall function as a CGI- or NSAPI-program (or corresponding) which shall receive messages which the service client 1 transmits.

The version field shall be controlled in order to see whether the service application 4 can manage the protocol. If the version control fails, the program shall return an error code in HTML-form. In other case the type of the message shall be controlled in order to see if verification and/or decryption must be performed. Verification/ decryption, if any, shall be performed, and if it succeeds, all parameters shall be transmitted to the product unique LADOK-code, otherwise the parameters, user identity, if any, and signature, if any, shall be logged. As person identifier shall be used civic registration number, if this is accessible on the smart card, in the certificate or in another safe place.

If there is no civic registration number on the card, authentication only can be made if there is a safe mapping between the certificates and the civic registration numbers, in for instance LADOK.

If the verification succeeds, it does not mean that the user is allowed to do what he/she likes in the system, but only that the identification is confirmed, so loggings, if any, of users who neglect their duties in LADOK must be made in the LADOK-system.

The following services shall be implemented:

- Show the five latest reported courses/moments. No inparameters. Returns at the most five courses (course code) and mark.
- Show status for a certain course. Inparameter course code, six characters. Returns mark for the course.
- Show sum of passed course points, No inparameters. Returns number of passed points, at the most four characters.
- Show certificate of studies to fax or printer. Inparameter fax number/printer number. Returns OK/error.

To the above it possibly can be necessary to include civic registration number. If a transaction code to map course code to course name is made accessible, the server will return course name instead of course code.

The code shall be possible to be run on machines with the operative systems UNIX or Windows NT and must not be depending on a special Web-server. However, it is sufficient if the system functions with a few different Web-servers (two or more). Parts of the code which are written uniquely for a certain operative system shall be documented separately to facilitate porting.

The application is programmed in such a way that it is easy to adapt the solution to new problems and should not

be written uniquely for LADOK. Parts which are unique to LADOK shall be divided into own source codes to facilitate reuse of the parts in common.

What has been described above is only to be regarded as an advantageous embodiment of the invention, and the scope of protection of the invention is only defined by what is indicated in the following patent claims.

PATENT CLAIMS

1. Device including a service client computer (1) and a WWW-browser at a telecommunications system or a data communications system which makes possible signing and encryption of information which is transmitted between a transmitting equipment and a receiving equipment, c h a r a c t e r i z e d in that a software for signing and encryption by means of software or smart cards is linked together with a software which shows text, data entry fields, buttons and icons, etc, which linked up program is arranged to be utilized as a plug-in unit or a Java-unit in said WWW-browser, at which all information to/from said service client computer (1) is decrypted/encrypted in said plug-in unit or said Java-unit.

2. Device according to patent claim 1, c h a r a c t e r i z e d in that said service client computer (1) includes a safety software (2) for verification of said signature.

3. Device according to patent claim 1 or 2, c h a r a c t e r i z e d in that said service client computer (1) is connected to a card reader, at which a user of said service client computer (1) identifies himself/herself by means of an active card together with a personal code, at which said active card includes a private key, which is needed for signing and encryption, and a certificate including a public key and personal data etc.

4. Method which utilizes a service client computer (1) and a WWW-browser at a telecommunications system or a data communications system for signing and encryption of information which is transmitted between a transmitting and a receiving equipment, c h a ra c t e r i z e d in that a

software for signing and encryption by means of smart cards or by means of software is linked together with a software which shows text, data entry fields, buttons and icons, etc, which linked up program is utilized as a plug-in unit or Java-unit in said WWW-browser, at which all information to/from a user of said service client computer (1) is decrypted/encrypted in said plug-in unit or said Java-unit.

5. Method for verification of a user of the service client computer (1) according to the patent claim 4, c h a r a c t e r i z e d in that it includes the steps that:

a) the user of the server client computer (1) creates a signed message by an API-call to the safety software (2), where said message is given as parameter, at which the service client computer (1) receives answer as "signed message" or "type of error".

b) if a signed message arrives at the service client computer (1) the message shall be packed into a structure and be transmitted over the WWW-network to a service application (4) via a Web-server (3) for the service client computer (1), at "type of error", the message is logged;

c) service application (4) disassembles the structure and transmits the user identity (AI) and the signed message to a safety software (5) for verification, at which the safety software (5) verifies the user or gives error code;

d) at verification the service application (4) transmits the message and user identity to the database (6) to which the service client (1) wants access; at error code user identity and message are logged.

e) the service application (4) receives verification answer from said database (6) and returns this answer to the service client computer (1) via the WWW-network;

f) the answer which said service client computer (1) receives is of a text/html-form or of MIME-type, whereby said plug-in unit or Java-unit starts in said WWW-browser in the service client computer (1).

6. Method according to patent claim 5, c h a r a c t e r i z e d in that said answer from said database (6) includes a description of how it shall be possible to extend information transmission for encryption in both directions.

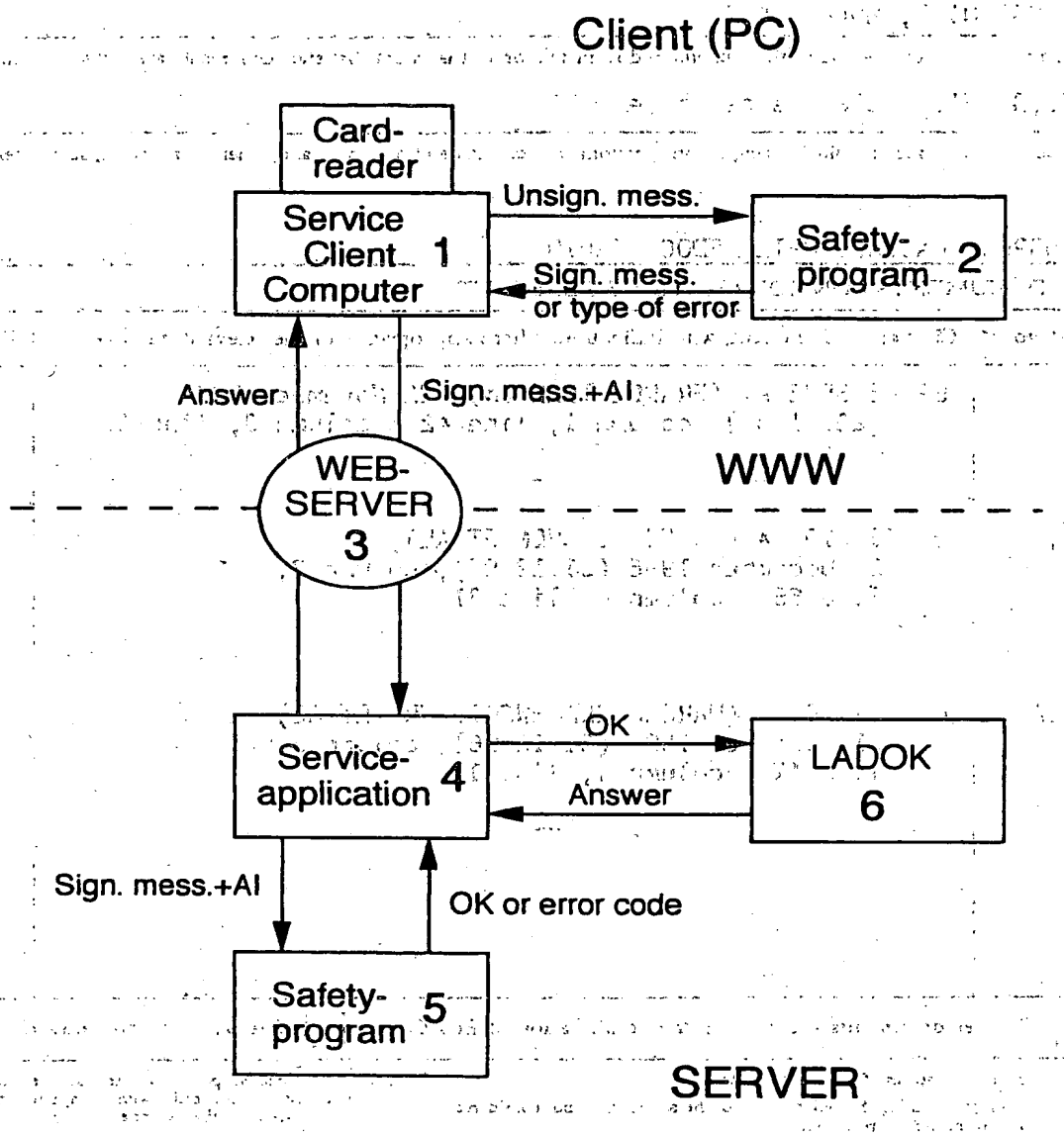


Figure 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 97/01713

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32, G06F 17/30, H04K 1/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04K, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

INSPEC, PASCAL, WPIL, EDOC, JAPIO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0683582 A1 (FRANCE TELECOM), 22 November 1995 (22.11.95), column 1, line 42 - column 3, line 27 --	1-6
P,A	US 5590197 A (JAMES F. CHEN ET AL), 31 December 1996 (31.12.96), column 3, line 65 - column 4, line 31 --	1-6
P,A	US 5590199 A (MARJAN KRAJEWSKI, JR. ET AL), 31 December 1996 (31.12.96), column 3, line 41 - column 4, line 13, --	1-6

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"B" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 March 1998	09 -03- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Anders Ströbeck Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 97/01713

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	US 5568554 A (DONALD E. EASTLAKE, 3RD), 22 October 1996 (22.10.96), column 3, line 21 - line 43	1-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

03/02/98

International application No.
PCT/SE 97/01713

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0683582 A1	22/11/95	FR 2720209 A,B	24/11/95
US 5590197 A	31/12/96	NONE	
US 5590199 A	31/12/96	NONE	
US 5568554 A	22/10/96	NONE	